Computer Forensics

Presented by

David Stenhouse
and Pamela Quinerto

Computer Forensics Inc.™
1749 Dexter Avenue North
Seattle, WA 98109
206-324-6232
dstenhouse@forensics.com
pquintero@forensics.com

Computer Forensics Inc.™ (CFI), a pioneer in the science of the forensic computing, combines the expertise of computer, litigation, and records management specialists. As Director of Operations for Computer Forensics Inc.™, David Stenhouse is responsible for the management of CFI's forensic specialists, technicians, and case managers. Representative computer forensic cases include product liability, trade secret theft, employment law, contractual disputes, electronic document authentication, bankruptcy, insurance claim disputes, intellectual property and shareholder class action, and antitrust litigation matters.

As a Computer Forensics Specialist at Computer Forensics, Inc.™, Pamela Quintero performs forensics procedures on a wide array of mass storage devices. Ms. Quintero has received training in forensics techniques from Guidance Software. Additionally, as the lab coordinator, she conducts a variety of analyses to evaluate hardware and software for use in the lab, overseeing scheduling, and maintaining the equipment in a "ready to go" condition.

The Expert's Role in Computer-Based Discovery

Joan E. Feldman, President
Computer Forensics Inc.™

Attorneys and judges can face extreme challenges to their technical knowledge when it comes to computer-based discovery. Locating, reviewing, and managing computer-based files requires an understanding of technology that often goes beyond that of the most experienced power user. In recent years, attorneys and the courts have turned to computer forensics experts for help in cutting through the technical issues that often cloud discovery objectives.

The computer forensics expert may fill one of two roles. The computer forensics expert may serve in the traditional role of the expert – helping to educate the court and all parties in their search for facts. In such cases, the expert may review the computer evidence directly and prepare forensic reports and affidavits, or oversee the work of the other party's expert witnesses. In a secondary role, the expert may act as more of a "vendor" of services. For example, the expert may not prepare an expert report of findings, but may instead provide a range of services such as consulting or project management tasks.

Because computer-based discovery is still relatively new, the type of services provided by forensics experts in a "vendor" role is often misunderstood. The following list of activities and services explains some of the common tasks handled by forensic experts. The choice of the appropriate computer forensics expert is also driven by counsels' objectives. For many of the tasks listed below, consulting and project management skills are as important as technical expertise.

Identification of Data Types for Review

In a consulting role, the expert can work to ensure that the attorney understands the various types of data available for review. The main categories of data: active, residual, and backup will determine how the data is collected and reviewed. Various data types are described below:

Active data

In addition to program and operating system files, the two categories of active data most commonly reviewed are:

1. *User created data*, readily available and accessible to users. User created data includes e-mail messages, word processing documents, spreadsheets, databases, electronic calendars, etc. Active e-mail messages can be read simply by opening a mailbox.

2. *System generated copies of user data*, not easily found or accessed by an average user. Such data includes copies of files created for the user by the application software or operating system. Common examples include temporary files created by Windows and stored in the "Temp" directory, and "near-copies" of files such as saved revised documents. E-mail, like Exchange Outlook, can automatically create entire archives of data. *See, for example, Microsoft Outlook's description of its archive function:*

   > "During installation, several folders are set up at with "AutoArchive" turned on. These folders and their default aging periods are Calendar (6 months), Tasks (6 months), Journal (6 months), Sent Items (2 months), and Deleted Items (2 months)."

Residual data

Includes "deleted" files that may still exist on a drive surface. When a file is deleted, the data in that file is not erased. Rather, the computer marks the file space as "free" and the file remains retrievable. Data in a deleted file is not erased until it is overwritten with data from a newly saved file or until it is "wiped" by specialized programs. Residual data can also include portions of files distributed on the drive surface or embedded within other files. These files are commonly referred to as "file fragments" and "unallocated" data.

Backup data

Information copied to portable media (usually tape) to provide users with access to their data in the event of a system failure. Networked systems are normally backed up on a routine schedule. Typical network backups capture only the data that are saved to the centralized storage systems (*e.g.,* the file server) and do not capture data stored on individual users' hard drives. PC users tend to selectively back up data onto floppy diskettes, tape, or removable hard drives.

Locating Responsive Data

In traditional discovery efforts, responsive documents can be found in locations throughout the business enterprise in many formats (file

cabinets, desk drawers, file repositories, microfilm/microfiche collections, etc.). Identifying and locating *responsive computer-based* documents requires that parties understand where to look
within the computing environment. The expert, in a consulting role, will help direct the parties in their review by first establishing what they are looking for (data types), then directing the parties to the appropriate data type location. Standard data locations include, but are not limited to, individual drives, shared drives, and backup tapes.

Individual Drives

Users may save their data on the drive of their desktop PC workstation or notebook computer. Floppy disk drives, Zip drives, or other drives may also be available and data can be copied to floppy diskettes, Zip cartridges, or tape at the desktop.

> *Note: Users generally store their files to the shared drive if they are on a networked system. Users can of course, store files in more than one location, i.e., on their hard drive as well as on the server. Drives normally contain active, archival, and residual data.*

Shared Drives

Shared drives**,** also referred to as network drives, file servers, etc., act as centralized data repositories for user data. A shared drive can be thought of as an electronic file room, with files indexed to facilitate access by individuals and groups. In most business environments, users save their work product (data) to a shared drive. Data created and saved may include:

- electronic mail
- word processing documents
- databases
- general ledger and accounting documents

Shared drives are usually managed centrally by an information services department.

> *Note: Shared drives usually contain active data only. If residual data exists on shared drives, the volume is minimal.*

Backup Tapes

Backup tapes contain copies of data stored on shared drives. Backup tapes rarely contain copies of data stored on individual drives.

> *Note: Backup tapes are often re-used or recycled. Recycling a backup tape is usually done on a rotation schedule. When a tape is re-used or recycled, data on the tape is overwritten by new data, effectively destroying the old data on the tape.*

Capturing Data in an Ex Parte Seizure

On occasion, computer forensic experts must go onsite to acquire evidence from network servers and/or hard drives without notice.

The forensic examiner's first task is to attempt to determine what types of computer systems are in use. For example, knowing the operating system(s) and tape drive(s) in use allows the examiner to bring appropriate software and hardware. As system details are rarely available, and the forensic expert often must rely upon informal or anecdotal information to prepare for the onsite data capture. This means that the expert must use a "kitchen sink" approach to packing appropriate materials, ensuring that a range of tape drives, controllers, software drivers, and media are included.

Another logistical concern is to ensure a law enforcement presence. Although many forensic examiners are former state or federal law enforcement agents, many are unwilling to go into a hostile environment without protection. U.S. Marshals commonly accompany attorneys and forensic specialists for ex parte seizures, and they usually remain during the entire evidence gathering process.

Once onsite, the forensic examiner may enlist the system administrator to provide technical information regarding file servers and workstations. Administrative cooperation is often won by virtue of necessity. It is the rare system administrator that wants to see outsiders opening drives and or attaching peripheral devices to their computer system. In most cases, the system administrator can help guide the process without endangering the chain of custody. Their cooperation will greatly speed up the work. It is here where an experienced forensic specialist can provide an advantage. A bullying or "police wannabe" stance adopted can easily double or triple the time and costs involved.

A full system backup is usually all that is required to capture all responsive data on the server(s). File servers manage and store deleted files and file fragments differently than individual hard drives, the necessity for creating a sector-by-sector copy (evidentiary image copy) of the drive surface is rarely required. The forensic specialist should observe the initiation of the backup process and should verify the

completeness and integrity of the backup. A full system backup can take 8 to 16 hours to complete. Once complete, the backup tape(s) should be write-protected and collected along with any other existing backup tapes that may contain responsive data.

Individual workstation computers (PC's) require a different type of capture. Evidentiary image captures differ from server backups using commercially available software. An evidentiary image backup copies and preserves all of the data on a hard disk, including inactive or "deleted" files.

The mechanics of the evidentiary backup are relatively simple. A cable is attached to the printer port or SCSI controller of the source computer. The opposite end of the cable is connected to a target drive (hard drive, JAZ, or tape drive). The source computer is "booted" up from the floppy drive, and the image capture software is also run from the floppy drive. No software is loaded onto the source computer at any time.

The majority of computer forensic specialists use software designed specifically to meet the highest level of evidentiary standards. Integrity of the image backup is rigidly enforced by means of cyclical redundancy checksums distributed throughout the backup process. An audit file is created during each image capture, documenting all events within the backup and restoration process. An average image backup takes between 1 to 12 hours, depending upon the size and speed of the source hard drive, choice of printer port or SCSI controller, and the type of target media used.

Once completed, the target drive is disconnected from the source computer, and removed for further review.

Reviewing Data

The expert's review of computer-based data may include a number of processes, such as the forensic capture and restoration of data, parsing out privileged data, re-creating database environments, re-creating electronic mail system environments, text-searching, and sorting data for review

Each review process is dependent upon the type of data to review, the location of the data, and the requirements of the parties. Hard drives, shared drives, and backup tapes all require particular processes, hardware, and software for review.

Data on Hard Drives

Hard drive review usually requires examining an evidentiary image copy of the drive, versus a direct examination of an in-use computer. Forensic experts use specialized software to create image copies. The image copy is then restored to a drive in a computer forensics lab for review.

In the lab, the expert can sort and analyze active, archival, and residual data in a number of different ways. The expert can use text-searching software to identify and sort selected words and phrases. A chronological sorting of files can be done in a matter of seconds. In cases where electronic mail is located on the hard drive (usually limited to the user's personal store file and/or archive), the electronic mail can be viewed in its native format or exported to text for review.

Experts review drives for content, but they also review drives to document user activity, looking for indications of file tampering, destruction, and patterns of use.

Data on Shared Drives

Shared drive review normally calls for the examination of a "snapshot backup," a backup session created specifically for the case. Snapshot backups are captured on drive or tape, and are processed in the same manner as other backup data.

Data on Backup Tapes

Before the data contained on backup tapes can be reviewed, it must first be restored to a drive. The restoration of data includes: configuring a server to run the appropriate operating system; installing the appropriate application software, backup software, and tape drive; scanning tapes to build a catalog or index for the backup session; and restoring the selected files from the backup tape.

If multiple backup sessions are restored and reviewed, there can be huge volumes of duplicative data. Duplicate data is normally redacted prior to review.

Once restored to a drive, the data is in an "active" state and can be reviewed for text, sorted chronologically, and examined as with any active file.

Special Issues re E-Mail Review

E-mail requires additional processing steps if multiple mailboxes are to be reviewed. These steps include: restoring the appropriate post offices, resetting user passwords, opening user mailboxes, redacting duplicate messages, and filtering or exporting the e-mail messages and attachments to text for searching with high speed text searching software.

Redacting Privileged Data

Computer forensic experts can ensure that privileged or confidential information does not get inadvertently disclosed. A neutral, or third party expert, generally takes on the task of assisting the parties with the location and redaction of privileged and/or confidential data.

Drives and tapes contain large volumes of data. This data is rarely divided into privileged/non-privileged categories. In the case of hard drives that contain archival and residual data, the chance for over-inclusion of non-responsive and privileged material is very high.

Computer forensics experts can help both parties reach a stipulation concerning the redaction of data, or the expert can follow the directions of the court. In either event, the expert will use the appropriate tools (usually text-searching capability) to identify non-responsive or privileged data. Once located, the responding party can review the selected files, and counsel can reach a determination of privilege.

The expert can assist counsel by preparing rudimentary privilege log indices, such as listing the source (file path), dates, and file names for redacted files. In the case of electronic mail, more detailed privilege logs can be prepared, using fielded data, such as “date”, “to”, “from”, “cc:”, and “subject line”.

Producing Data

The final stage in the expert’s process is the output of responsive data. The expert can provide the attorney with electronic versions of data, usually “burned” to CDs. Data on CDs cannot be modified, and provides an assurance of data integrity greater than that of data saved to hard drives or tape. Electronic files can also be turned into “TIF” images (the equivalent of an electronic photocopy), and the images may be placed onto CD, drives, or tape. Finally, the parties may also request paper printouts of data files in lieu of or in addition to documents in an electronically stored format.

Generally, the objective of the parties is to gather data and review it for privilege prior to production. Before starting this process, it is important for all parties to understand that questions of timing and cost will be predicated upon the data set to be reviewed and the method(s) used for review.

Attorneys need to understand that the volume of electronic data cannot be predicted in advance. Like Russian dolls or icebergs, huge volumes of data may hide under the surface. Information about the volume of data to be processed is usually only revealed after processing and restoration has begun. A cursory examination and selection of data can hide significant facts. For example, a backup tape may appear to contain only a hundred files. This may seem like a negligible amount of data to review until the 100 files are revealed to be “ghost” copies of hard drives – with each hard drive containing tens of thousands of files.

As the expert works with the attorneys, lines of communication must be constant and open at all times. Each fact revealed during the restoration and review process will lead to decision requirements. For example, if the data collection is double or triple the volume expected, the attorney will need to determine whether to push forward for a review of all data or decide to make selections based upon other criteria. It is not uncommon for attorneys to decide to limit their review to relevant text, or a certain time frame, data location, or data type in the face of potentially large costs or looming court deadlines.

Determining the role of the computer forensics expert ("traditional expert" vs. "service provider" or vendor) is an important first step in any case. A qualified computer forensics expert should be prepared to help educate and navigate attorneys through the entire examination and production process. The expert should also keep the parties apprised during the entire review process and help guide them towards workable results. Most computer-based discovery efforts require adequate equipment, technical skills, and project management expertise. A focus on the "end game" or final objectives will help guide the attorney to the correct expert for the job.

Top Ten Things To Do When Collecting Electronic Evidence

Joan E. Feldman, President
Computer Forensics Inc.™

It is now black letter law that information generated and stored on computers and in other electronic forms is discoverable.[1] It is estimated that as much as 30 percent of the information stored on computers is never reduced to printed form. Moreover, the electronic version of a document usually contains information that simply does not appear in the printed version.[2] As a practical matter, finding the information stored on computers is becoming an important part of the discovery process.

Many lawyers now ask for electronic evidence, especially e-mail, as a routine part of their discovery efforts. But, as a practical matter, most lawyers have little or no experience in collecting and analyzing the data

[1] See *Anti-Monopoly, Inc. v. Hasbro, Inc.*, 94 Civ. 2120, 1995 U.S. Dist. LEXIS 16355 (S.D.N.Y. 1995)("Today it is black letter law that computerized data is discoverable if relevant."); *Santiago v. Miles*, 121 F.R.D. 636, 640 (W.D.N.Y. 1988) ("A request for raw information in computer banks is proper and the information is obtainable under the discovery rules."); *In re Brand Name Prescription Drug Antitrust Litigation*, 94-C-987, M.D.L. 997 (N.D. Ill. 1995) (e-mail is discoverable); *Seattle Audubon Society v. Lyons*, 871 F. Supp. 1291 (W.D. Wash. 1994) (ordering production of e-mail).

[2] This fact is also well recognized by most courts. See *Public Citizen, Inc. v. Carlin*, Civil Action No. 96-2840 (PLF) (D.D.C. Oct. 22, 1997) ("electronic records often contain information not preserved in a print-out record or even in other computerized systems of records."); see also *Armstrong v. Executive Office of the President,* 1 F.3d 1274 (D.C. Cir. 1993).

they request. This article provides practical advice on how to collect the relevant data and how to assure that data collected can be authenticated and admitted as evidence.

1. Send a preservation of evidence letter. Because the information stored on computers changes every time a user saves a file, loads a new program, or does almost anything else on a computer, it is critical that you put all parties on notice that you will be seeking electronic evidence through discovery. The sooner the notice is sent the better. The notice should identify as specifically as possible the types of information to be preserved and explain the possible places that information may exist.[3] If necessary, obtain a protective order requiring all parties to preserve electronic evidence and setting out specific protocols for doing so.

2. Include definitions, instructions, and specific questions about electronic evidence in your written discovery. This is a continuing process, with three objectives to accomplish:

First, use a series of interrogatories to get an overview of the target computer system. These interrogatories will be followed up by a 30(b)(6) deposition of the Information Systems department.

Second, all requests for production should make clear that you are requesting electronic documents as well as paper. You can do this through defining documents to include items such as data compilations, e-mail, and electronically stored data. You should also draft requests that specifically ask for different types of computer-based evidence such as diskettes, e-mail, and backup tapes.

Finally, if necessary, include a request for inspection so you can examine the computer system first hand and retrieve any relevant data.

3. Take a 30(b)(6) deposition of the Information Systems department. This is the single best tool for finding out the types of electronic information that exists in your opponent's computer systems.

[3] Courts are willing to impose discovery sanctions when electronic records are altered or destroyed. See *Computer Assoc. Internat'l v. Am Fundware*, 135 F.R.D. 166 (D. Colo. 1990); *Nat'l Assoc. of Radiation Survivors v. Turnage*, 115 F.R.D. 543 (N.D. Cal. 1987). Sanctions may be imposed even when the alteration or destruction occurs in the regular course of business. The common thread in the cases imposing sanctions is the fact that the party altering or destroying its computer records was on notice that such records were relevant to pending or threatened litigation.

Checklist For System Discovery

- ❑ The layout of the computer system, including the number and types of computers, and the types of operating systems and application software packages used. When asking about any types of software, make sure to ask for the software maker, program name, and version of each program (*e.g.*, Corel, WordPerfect, version 6.0).
- ❑ The structure of any electronic mail system, including software used, the number of users, the location of mail files, and password usage.
- ❑ The structure of any network, including the configuration of network servers and workstations, and the brand and version number of the network operating system in use.
- ❑ Specific software used. This includes software applications for things such as calendars, project management, accounting, word processing, and database management. It also includes industry-specific programs, proprietary programs, encryption software, and utility programs. When asking about software, inquire when software was installed and when it was upgraded.

- □ The personnel responsible for the ongoing operation, maintenance, expansion, and upkeep of the network.
- □ The personnel responsible for administering the e-mail system.
- □ The personnel responsible for maintenance of computer-generated records and the manner in which such records are organized and accessed.
- □ Backup procedures used on all computer systems in the organization. This should include descriptions of all devices (*e.g.*, tape drives) and software used to create backups, the personnel responsible for conducting the backups, what information is backed up, backup schedules, and tape rotation schedules.
- □ The process for archiving and retrieving backup media both on and off site.
- □ The procedures used by system users to log on to computers and into the network. This includes use of passwords, audit trails, and other security measures used to identify data created, modified, or otherwise accessed by particular users.
- □ Whether and how access to particular files is controlled. Information such as access control lists identify which users have access to which files.
- □ How shared files are structured and named on the system.
- □ Routines for archiving and purging different types of data.

4. **Collect backup tapes.** One of the most fertile sources of evidence is the routine backup created to protect data in case of disaster. This information is normally stored on high capacity tapes, but may exist on virtually any type of media. Backup tapes normally contain all an organization's data, including e-mail, as of a certain date. Common backup procedures call for full backups to be made weekly, with the last backup of the month saved as a monthly backup. While weekly backups are normally rotated, monthly backups are saved anywhere from six months to several years. It is not unheard of for an organization to have kept all its backup tapes from the inception of its computer systems.

When collecting backup tapes in discovery, make sure to also gather information on how the tapes were made. This inquiry must include both the procedures followed and the specific hardware and software used to make the backups. Because, over time, hundreds of different backup programs and equipment have been used, in some cases, it may be impossible to restore backups without using the same software and/or hardware used to create them.

5. Collect removable media. Data selectively saved by users to diskettes or other portable media is another fertile, but often overlooked, source of evidence. Users save data to diskettes for any number of reasons. Users create "ad hoc backups" of key documents or files to use in case an important document or file is lost. Users may also copy e-mail files to diskette to prevent them from being deleted in automatic purging routines. Finally, users will use diskettes to save data they do not want to keep on company computers.

Diskettes are saved indefinitely by the users that create them. It is not unusual to find a number of diskettes in witness's desks. Collecting and examining all diskettes created by key witnesses is an essential step in a thorough examination of all electronic evidence.

6. Ask every witness about computer usage. In addition to the discovery directed at the computer system, every witness must be questioned about his or her computer use. Individual users' sophistication varies widely. Knowing how each witness uses his or her computer, and organizes and stores data, may lead to sources of data not revealed by the discovery directed at general system usage. This discovery should also focus on the secretaries and other people assisting key witnesses. Often, documents drafted by the key witness are stored on his or her assistant's computer.

Perhaps the most overlooked source of electronic evidence is the home computer. Data usually ends up on home computers in one of two ways. First, data can be transferred to and from the workplace on diskettes or other portable media. Second, an employee may be able to log on to the company network from home. In this situation, the home computer acts just like the employee's office workstation. Regardless of how data is transferred, the critical point is to find out whether the witness works from home and how data is transferred to and from that home computer.

Palmtop devices and notebook computers are another good source of evidence. Palmtop devices include electronic address books as well as more powerful devices such as 3Com's Palm Pilot and Apple's Newton. In addition to storing calendar and contact information, many of these devices allow users to make notes and use e-mail. Further up the scale, there are notebook computers. Notebook computers are often shared among a number of users. While the notebook computer may not be a witness's primary workstation, it still may contain important pieces of information. Again, the critical point is to ask how palmtop devices and notebook computers are used and what data they may contain.

7. Make image copies. It is no secret that deleted files and other "residual" data may be recovered from hard drives and floppy disks. How do you make sure that you capture this data? Answering this question first requires a brief explanation of why "residual" data exists.

When working with computers, the term "deleted" does not mean destroyed. Rather, when a file is deleted, the computer makes the space occupied by that file available for new data. Reference to the "deleted" file is removed from directory listings and from the file allocation table, but the bits and bytes that make up the file remain on the hard drive until they are overwritten by new data or "wiped" through use of utility software. The result is that a file appears to have been deleted, but may still be recovered from the disk surface.

Residual data includes "deleted" files, fragments of deleted files, and other data that is still extant on the disk surface. To assure that this residual data is captured, you must make an image copy of the target drive. An image copy duplicates the disk surface sector-by-sector, thereby creating a mirror image of the target drive. In contrast, a file-by-file copy (what is made when you simply select the files you want copied) captures only the data contained in the specific files selected. Even if all files are selected, a file-by-file copy will not capture any residual data.[4]

[4] When collecting computer data for evidentiary purposes, a party has a duty to "utilize the method which would yield the most complete and accurate results." *Gates Rubber Co. v. Bando Chemical Indus. Ltd.*, 167 F.R.D. 90, 112 (D. Colo. 1996). In *Gates*, the court criticized the plaintiff for failing to make image copies and for failing to properly preserve undeleted files.

Electronic Media Collection Checklist

Data Files*

- □ office desktop computer/workstation
- □ notebook computer
- □ home computer
- □ computer of personal assistants/secretary/staff
- □ palmtop devices
- □ network file servers/mainframes/minicomputers

**To assure that all data, including residual data, is captured, an image copy is recommended when copying data from local computer hard drives.*

Backup Tapes

- ❑ system-wide backups (monthly/weekly/incremental)
- ❑ disaster recovery backups (stored off site)
- ❑ personal or "ad hoc" backups (look for diskettes and other portable media)

Other Media Sources

- ❑ tape archives
- ❑ replaced/removed drives
- ❑ floppy diskettes and other portable media (*e.g.*, CDs, Zip cartridges)

8. **Write protect and virus check all media.** Now that you have obtained the data, how do you look at it? You likely have a mix of image copies, backup tapes, diskettes, CDs, and other media. Before doing anything else, you must maintain the integrity of the media you have received. The two key steps in doing this are write protection and virus checking.

Write protecting media prevents data from being added to that media. Write protecting the media produced guarantees that the evidence you gather is not altered or erased when you are working with it. You should write protect all media before doing anything else with it. The process for write protecting media varies, but is usually fairly simple.

Virus checking, likewise, prevents evidence from being altered and is the second thing you should do with all media. The key is using up-to-date virus checking software. If a virus is detected, record all information about the virus detected and immediately notify the party producing the media. Do not take steps to clean the media, because doing so would change the evidence that was produced to you.

9. **Preserve the chain of custody.** A chain of custody tracks evidence from its original source to what is offered as evidence in court. With electronic evidence, a chain of custody is critical because electronically stored data can be altered relatively easily, and proving the chain is the primary tool in authenticating electronic evidence.

Preserving a chain of custody for electronic evidence, at a minimum, requires proving: (a) no information has been added or changed, (b) a complete copy was made, (c) a reliable copying process was used, and (d) all media was secured. Write protecting and virus checking all media are the key steps in meeting the first requirement in preserving the chain and making image copies is the key step in meeting the second.

A reliable copy process has three critical characteristics. First, the process must meet industry standards for quality and reliability. This includes the software used to create the copy and the media on which the copy is made. A good benchmark is whether the software is used and relied on by law enforcement agencies. Second, the copies made must be capable of independent verification. In short, your opponent and the court must be able to satisfy themselves that your copies are accurate. Third, the copies created must be tamper proof.

Securing the media simply assures that your original copies are preserved. Just as you would make working copies of any documents produced, you should create working copies of data.

When you work with data restored from the media you collected, make sure you can track individual files and documents back to their original source. The checklist below sets out one way of doing this.

Checklist For Electronic Media Examination

- ❑ Assign a unique number to each piece of media. (The number series used for numbering electronic media should be distinct from that used for paper documents.)
- ❑ Write protect all media.
- ❑ Virus check all media. Record any viruses discovered and immediately notify the producing party.
- ❑ Print directory listings for each piece of media. Make sure the listing has the media number printed on it.
- ❑ Virus check the drive that you are restoring the data to and make sure the drive is free from any other data. (Restoration should be to a distinct drive, dedicated to a single case.)
- ❑ Restore each piece of media to a file with a name that corresponds to the number assigned to the media being restored (*e.g.*, a diskette numbered 123 should be restored to a file named “Disk 123”).
- ❑ Verify that all files on the directory listing appear in the copy restored.
- ❑ Secure the source media.
- ❑ When printing a particular document, insert a distinct header or footer that gives the full directory listing for document printed (*e.g.*, Disk 123\corr\smokinggun.txt).

10. **Hire an expert.** There are many reasons that you should consider retaining an expert to assist in your electronic discovery.[5] The reasons to hire an expert and the qualifications to look for in that expert include:

- An expert should have the experience and the equipment to handle the diverse array of software and hardware you will inevitably encounter. The combinations of hardware and software used to create, store, manipulate, and communicate data are growing daily. An expert will help you navigate through this maze to get what you need – the evidence.
- An expert can help fine tune your discovery and maximize the amount of relevant data you recover.
- An expert provides resources for copying and examining data being produced. For example, restoring backup tapes and image copies takes large amounts of drive space (unused computer memory) – far more space than most lawyers or their clients have available.
- An expert should have the tools and skills to search the data you obtain for the evidence relevant to your case.
- An expert should be able to perform forensic analysis and help recover residual data and other hidden or lost data.
- An expert will help preserve chains of custody and help prove authenticity. Retaining an expert to collect and analyze electronic evidence removes you from the potentially difficult position of having to testify about the authenticity and accuracy of this evidence.

Conclusion. With the ever-growing use of computers as business and communication tools, data generated, and stored electronically are becoming an increasingly important target for discovery. As with all other discovery, the goal in the discovery of electronic information is finding useful information and collecting that information in a manner that assures it can be admitted into evidence. There is no magic to accomplishing this goal – what is required as a proven, methodical approach. While technology will undoubtedly continue to change, the basic techniques for collecting electronic evidence should continue to prove effective.

[5] In *Gates Rubber Co.*, the court discussed its impressions of the parties' computer expert and technician. It was clear from the discussion, that the court placed more credibility on the evidence and arguments supported by the work of the expert. 167 F.R.D. at 112.

Resources & Further Reading

General

Computer Forensics Inc.™
http://www.forensics.com

Electronic Evidence & Records Retention Page
http://www.willyancey.com/electronic_evidence.htm

Computers and Law™
http://wings.buffalo.edu/Complaw/

Links to Articles
http://www.kenwithers.com/articles

How Much Information is Generated Today
http://www.sims.berkeley.edu/research/projects/how-much-info/index.html

An Attorney’s Guide to Protecting, Discovering and Producing Electronic Information
Michael J. Patrick, Fenwick & West
Publisher: LRP Publications
1-800-341-7874

E-Mail Essentials (video)
Produced by Quality Media Resources
Distributed by Computer Forensics Inc.™

Metadata

Microsoft Support Article Q223790
http://support.microsoft.com/support/kb/articles/Q223/7/90.ASP

Confidentiality and MetaData in Documents
http://www.addbalance.com/usersguide/metadata.htm

Ethics

"A Question of Ethics," by Clinton Wilder and Joan Soat
Information Week, February 19, 2001
http://www.informationweek.com/825/ethics.htm

Security

"In-House Cyber Security. Corporate Counsel Must Plan Ahead to Minimize Risks of Data Security Breaches," by Marc J. Zwillinger, Kirkland & Ellis
Legal Times, February 21, 2001

Federal Rules of Civil Procedure

Rule 26(b)	Scope of disclosure
Rule 30(b)(6)	Custodian of records deposition
Rule 34(a)	Defines discoverable documents
Rule 45(a)(1)(C)	Subpoena for tangible things (e.g., laptops)

Electronic Media Collection Checklist

Data Files*

- ❑ office desktop computer/workstation
- ❑ notebook computer
- ❑ home computer
- ❑ computer of personal assistants/secretary/staff
- ❑ palm-top devices
- ❑ network file servers/mainframes/minicomputers

*To assure that all data, including residual data, is captured an image copy is recommended when copying data from local computer hard drives.

Backup Media

- ❑ system-wide backups (monthly/weekly/incremental)
- ❑ disaster recovery backups (stored offsite)
- ❑ selective backups
- ❑ personal or “ad hoc” backups (look for diskettes, tapes, etc.)

Miscellaneous

- ❑ tape archives
- ❑ replaced/removed drives
- ❑ floppy diskettes and other portable media (e.g. CDs, Zip cartridges)

Sample Language for 30(b)6 Deposition of Custodian of Electronic Records

(Redacted from full version)

System Profile

1. Describe the types of computer system(s) used by your company in the course of business.

2. Describe/identify the type of software used on your computer system(s).

3. Identify the person(s) responsible for the ongoing operation, maintenance, expansion, backup, and upkeep of the computer system.

4. Does the staff [*or inquire after key witnesses*] have home computers used for business purposes? (If yes, repeat questions 1-2).

5. Are passwords or encrypted files used on any of the computer systems? If yes:

    5.1 Describe how files are protected.
    5.2 Who could provide access codes if required?

6. Have you modified your use of computers to comply with recent discovery requests?

Backup and Retention

7. List all computer systems in the organization that are backed up.

    7.1 Describe the backup program(s) used. (Ex: ARCserve, StorageExpress, Maynard, Tecmar, etc.)
    7.2 Give details of your backup procedures.

8. Have you modified your backup procedures to comply with recent discovery requests?

9. Are files ever deleted from the computer system(s)?

10. Are archival backups ever created? If yes:

10.1 What files have been archived?
10.2 Where are the archival backups maintained?

11. Describe any disaster recovery plans in place now and for the relevant time period.

Maintenance and Access

12. Are utility programs used on computer(s) in the office? (Ex: Norton Utilities, MacTools, network maintenance programs) If yes:

12.1 Which program(s)?
12.2 Has the program been used to permanently “wipe” files? (When?)
12.3 Has the program been used to de-fragment, optimize, or compress drives?
(When?)

13. How do those outside of the company access the computers?

14. How are office computers secured?

15. Has any computer hardware been upgraded in the past 12 months?

16. Has any computer software been upgraded or replaced on office computers in the past 12 months?

Chain of Custody/Authentication

17. Are individual directories purged when an employee leaves the company?

18. Are passwords and access codes revoked when an employee leaves the company?

19. Are workstations reassigned to incoming employees? If yes:

19.1 Are hard drives wiped or re-formatted for the new user?
19.2 Are hard drives backed up before the new user takes system?

20. Describe how used or replaced equipment is disposed of or sold.

21. Describe how used disks or drives are treated before destruction or sale. (Degaussed? Shredded?)

22. Have you used outside contractors to upgrade either hardware or software?
(If so, please identify.)

23. Are changes or modifications made to software recorded?
(Electronically? Are hard copy logs kept?)